

Data-protecting microprocessor circuit for portable record carriers, for example credit cards.

特許公報番号 DE4115152
 公報発行日 1992-11-12
 発明者: WEIKMANN FRANZ DR (DE)
 出願人 GAO GES AUTOMATION ORG (DE)
 分類:
 一国際: G06F12/14; G06K19/073; G07F7/10; G06F12/14;
 G06K19/073; G07F7/10; (IPC1-7): G06F12/14; G06K19/07
 一欧州: G07F7/10D10M; G06F12/14C1B
 出願番号 DE19914115152 19910508
 優先権主張番号: DE19914115152 19910508

他の公開

- EP0512542 (A2)
- JP5173890 (A)
- EP0512542 (A3)
- EP0512542 (B1)
- ES2100249T (T3)

ここにデータエラーを報告してください

下記の要約はありません DE4115152

対応特許の要約 EP0512542

In this microprocessor circuit, a protective circuit is provided which prevents access to unauthorised memory areas, particularly when so-called user programs are executed. The protective circuit is decoupled from the actual microprocessor circuit, but is preferably provided on the integrated circuit accommodating the microprocessor.

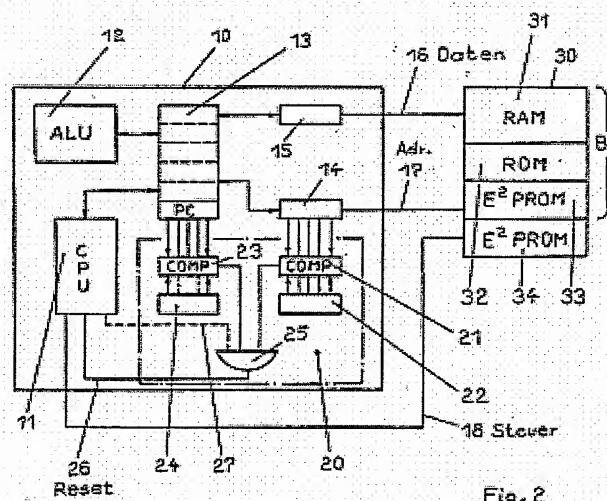


Fig. 2

esp@cenet データベースから供給されたデータ - Worldwide

パテントファミリーリスト

13 family members for: **DE4115152**

9 の出願から派生

[戻る DE4115152](#)

- 1 Data-protecting microprocessor circuit for portable record carriers, for example credit cards.
公報情報: **AT148953T T** - 1997-02-15
- 2 Data-protecting microprocessor circuit for portable record carriers, for example credit cards.
公報情報: **DE4115152 A1** - 1992-11-12
DE4115152 C2 - 2003-04-24
- 3 No title available
公報情報: **DE59208026D D1** - 1997-03-27
- 4 Data-protecting microprocessor circuit for portable record carriers, for example credit cards.
公報情報: **DK512542T T3** - 1997-08-18
- 5 Data-protecting microprocessor circuit for portable record carriers, for example credit cards.
公報情報: **EP0512542 A2** - 1992-11-11
EP0512542 A3 - 1993-08-11
EP0512542 B1 - 1997-02-12
- 6 Data-protecting microprocessor circuit for portable record carriers, for example credit cards.
公報情報: **ES2100249T T3** - 1997-06-16
- 7 Data-protecting microprocessor circuit for portable record carriers for example credit cards
公報情報: **HK1007818 A1** - 1999-04-23
- 8 DATA PROTECTING MICROPROCESSOR CIRCUIT FOR PORTABLE DATA CARRIER
公報情報: **JP3529800B2 B2** - 2004-05-24
JP5173890 A - 1993-07-13
- 9 Data protective microprocessor circuit for portable data carriers, for example credit cards
公報情報: **US5600818 A** - 1997-02-04

esp@cenet データベースから供給されたデータ - Worldwide



⑯ BUNDESREPUBLIK
DEUTSCHLAND



DEUTSCHES
PATENT- UND
MARKENAMT

⑯ **Patentschrift**
⑯ DE 41 15 152 C2

⑯ Int. Cl.⁷:
G 06 F 12/14
G 06 K 19/07

DE 41 15 152 C2

- ⑯ Aktenzeichen: P 41 15 152.6-53
 ⑯ Anmeldetag: 8. 5. 1991
 ⑯ Offenlegungstag: 12. 11. 1992
 ⑯ Veröffentlichungstag der Patenterteilung: 24. 4. 2003

Innerhalb von 3 Monaten nach Veröffentlichung der Erteilung kann Einspruch erhoben werden

⑯ Patentinhaber:

GAO Gesellschaft für Automation und Organisation mbH, 81369 München, DE

⑯ Vertreter:

Klunker, Schmitt-Nilson, Hirsch, 80797 München

⑯ Erfinder:

Weikmann, Franz, Dr., 81675 München, DE

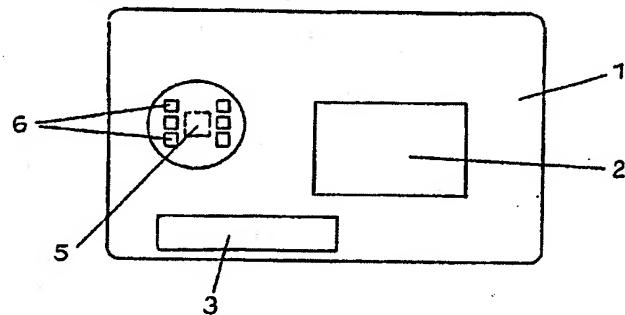
⑯ Für die Beurteilung der Patentfähigkeit in Betracht gezogene Druckschriften:

DE 39 01 457 C2

Patent Abstracts of Japan, P-14, 1980, Vol. 4, Nr. 78, JP 55-42 312 A;

⑯ Kartenförmiger Datenträger mit einer datenschützenden Mikroprozessorschaltung

⑯ Kartenförmiger Datenträger mit datenschützender Mikroprozessorschaltung zur Verhinderung des Zugriffs auf in Speichern abgelegten Daten oder Programmen mit einem Arbeitsprozessor, einem Speicher für ein Betriebssystem und mehreren Speicherbereichen zur freien Programmierung mit jeweils einem individuellen Fremdprogramm, mit einer Schutzschaltung, bestehend aus einer ersten Einrichtung zur Überwachung der jeweils gültigen Zugriffssadresse, einer zweiten Einrichtung zur Überwachung des jeweiligen Inhalts des Arbeitsprozessor-Programmzählers und einer dritten Einrichtung, die die Signale der Überwachungseinrichtungen zur Erzeugung eines Sperrssignals verknüpft, dadurch gekennzeichnet, daß die Schutzschaltung ein zweiter Mikroprozessor ist, der mit der gleichen oder einer höheren Taktfrequenz betreibbar ist als der Arbeitsprozessor.



DE 41 15 152 C 2

1

Beschreibung

[0001] Die Erfindung betrifft einen kartenförmigen Datenträger mit einer datenschützenden Mikroprozessorschaltung gemäß dem Oberbegriff des Anspruchs 1.

[0002] Mikroprozessorschaltungen der genannten Art finden bevorzugt Anwendung in sogenannten Chipkarten, d. h. Ausweiskarten, Kreditkarten, Buchungskarten und dergleichen, die mit einem integrierten Schaltkreis ausgestattet sind. Die Mikroprozessorschaltungen sind aber auch in so genannten Zahlungsverkehrsmodulen einsetzbar, die mit den obengenannten Karten über entsprechende Schnittstellen kommunizieren.

[0003] Um das Verständnis der Erfindung zu erleichtern, soll sich die folgende Beschreibung auf die Anwendung der Mikroprozessorschaltung bei Karten beziehen.

[0004] Eine Karte mit Mikroprozessor wurde erstmals in der DE-OS 27 38 113 beschrieben. Einer der wesentlichen Vorteile einer solchen Karte besteht in der vielfältigen Verwendungsmöglichkeit seitens des Karteninhabers. Der im integrierten Schaltkreis der Karte enthaltende Mikroprozessor und die dazugehörigen Speichermittel erlauben eine umfangreiche Datenverarbeitung in der Karte selbst, wohingegen die beispielsweise mit Magnetstreifen versehenen Karten es erforderlich machen, sämtliche Datenverarbeitungsvorgänge extern durchzuführen.

[0005] Der Kartenhersteller kann den Mikroprozessor mit einem fest gespeicherten Betriebssystem ausstatten, welches grundlegende Funktionen übernimmt, beispielsweise Prozeduren zum Vergleichen eines extern eingegebenen Codes mit einem gespeicherten Code und dergleichen. Die zu dem Mikroprozessor gehörigen Speicher dienen außer zur Absicherung des Betriebssystems auch zum Abspeichern bestimmter Anwendungen und Parameter, die z. B. zur Sicherheitsüberprüfung notwendig sind und auf jeden Fall geheimgehalten werden müssen.

[0006] Eine vielseitige Anwendung der Karten erreicht man dann, wenn man von einem Betriebssystem mit zugehörigen Programmen ausgeht, gewisse Schnittstellen definiert und einen Speicher oder Speicherbereich für ein sogenanntes Fremdprogramm reserviert. Der Kartenhersteller stellt dann für die Anwender, d. h. für die Karten ausgebenden Organisationen, einen Speicher bzw. Speicherbereich zur Einprogrammierung ihres Fremdprogramms zur Verfügung. In diesem Fremdprogramm kann die Organisation dann spezifische Operationen festlegen, die unabhängig vom Betriebssystem sind und die lediglich die spezielle Organisation betreffen.

[0007] Eine weitere denkbare Variante besteht darin, daß nicht nur eine einzige Organisation ihr Fremdprogramm in die vorgefertigte Chipkarte einprogrammiert, sondern daß mehrere unterschiedliche Organisationen ihre entsprechenden Programme einspeichern.

[0008] In jedem Fall muß dafür gesorgt werden, daß sicherheitsrelevante Daten, die Bestandteil des Betriebssystems oder auch der einzelnen Fremdprogramme sind, vor unbefugtem Zugriff geschützt werden.

[0009] Die JP 55-42 312 A befaßt sich mit dem Problem, daß beim Beschreiben von Speicherbereichen tatsächlich nur die beabsichtigten Speicherbereiche und nicht etwas andere Speicherbereiche beschrieben werden sollen. Dazu werden einerseits der Programmzähler, also die beabsichtigte Schreibadresse, und andererseits die tatsächliche beschriebene Speicheradresse überwacht, und zwar werden sie konkret darauf überwacht, ob sie beide in demselben vorgegebenen Adressenbereich liegen.

[0010] Der Erfindung liegt die Aufgabe zugrunde, die bekannte Schaltung im Sinne höherer Flexibilität zu modifizie-

2

ren.

[0011] Die Aufgabe wird durch die in den Ansprüchen 1 und 6 angegebenen Merkmale jeweils gelöst.

[0012] Die datenschützende Schaltung besteht aus einer ersten Einrichtung zur Überwachung der jeweils angesprochenen Adresse, einer zweiten Einrichtung zur Überwachung des Mikroprozessor-Programmzählers sowie einer weiteren Einrichtung, die die Signale der Überwachungseinrichtungen zur Erzeugung eines Sperrsignals verknüpft.

[0013] Durch die Überwachung des Programmzählerstandes ist die Schutzschaltung jederzeit in der Lage festzustellen, welches der geladenen Programme gerade ausgeführt wird. Bei gleichzeitiger Überwachung der vom jeweils aktiven Programm aufgerufenen Adresse kann über die Verknüpfungsschaltung auf einfache Weise auf einen nicht zulässigen Speicherzugriff reagiert werden, indem beispielsweise ein Reset-Signal auf den Mikroprozessor geführt wird.

[0014] Die Schutzschaltung ist vom eigentlichen Mikroprozessor entkoppelt, aber vorzugsweise auf dem den Mikroprozessor aufnehmenden integrierten Schaltkreis vorgenommen. Durch die Vorgabe entsprechender Sollwerte für den jeweiligen Programmzählerstand und die jeweiligen Adressen lassen sich beliebige Speicherbereiche definieren, die für einen bestimmten Anwender zulässig bzw. nicht zulässig sind. Sollen bestimmte Speicherbereiche selektiv bezüglich des Lesens oder Schreibens gesperrt werden, so ist das Schreib-/Lesesignal des Mikroprozessors in der Schutzschaltung entsprechend mit zu verarbeiten.

[0015] Die Erfindung sieht vor, daß die Schutzschaltung durch einen als Sicherungsprozessor bezeichneten Mikroprozessor ausgebildet ist, der den die Fremdprogramme ausführenden als Arbeitsprozessor bezeichneten Mikroprozessor überwacht. Durch diese Maßnahme steht der Arbeitsprozessor unter ständiger Kontrolle des Sicherungsprozessors, der nach jedem Reset und der darauffolgenden Initialisierungsphase den Betrieb des Arbeitsprozessors frei gibt. Stellt der Sicherungsprozessor fest, daß der ein bestimmtes Fremdprogramm ausführende Arbeitsprozessor auf einen nicht zulässigen Speicherbereich zugreift, so gibt der Sicherungsprozessor ein Sperrsignal auf einen nichtmaskierten Interrupteingang oder den Reset-Eingang des Arbeitsprozessors.

[0016] Da der Sicherungsprozessor sämtliche Einzelschritte des Arbeitsprozessors überwachen soll, wird er zweckmäßigerverweise mit einer höheren Taktfrequenz arbeiten als der Arbeitsprozessor.

[0017] Wenn in dem dem Arbeitsprozessor zugeordneten Speicher mehrere Fremdprogramme gespeichert sind, muß ein Zugriff nicht nur zum Betriebssystem, sondern auch zu anderen Fremdprogrammen verhindert werden. Die dazu notwendigen Sollwerte werden zweckmäßigerverweise in einem dem Sicherungsprozessor zugeordneten Speicher als Grenzwerte eingespeichert. Dazu ist dem Sicherungsprozessor ein Grenzwertspeicher zugeordnet, in welchem die Grenzwerte für die überwachten Adressen und für die möglichen Inhalte des Programmzählers des Arbeitsspeichers abgelegt sind. Auf diese Bereiche hat der Arbeitsprozessor keine Zugriffsmöglichkeit.

[0018] Das Sperren der Ausführung eines Fremdprogramms bei unberechtigtem Speicherzugriff kann auch dadurch erreicht werden, daß nur ein bestimmter Satz von interpretierbaren Befehlen zugelassen wird. Die Befehle des Fremdprogramms werden dann unter der Kontrolle des Betriebssystems ausgeführt, wobei gewährleistet ist, daß ein Zugriff nur auf solche Bereiche stattfindet, auf die ein Zugriff ausdrücklich zugelassen ist. Der Programmzähler des Mikroprozessors gelangt so nie unter die Kontrolle des

Fremdprogramms.

[0019] Neben den oben angesprochenen Möglichkeiten sieht die Erfindung in einer weiteren Variante vor, daß mehrere frei programmierbare Speicherbereiche vorgesehen sind, deren Adreßräume bis auf wenigstens eine höchstwertige Stelle gleich sind. Die jeweils höchstwertige, einem Speicherbereich zugeordnete Stelle, wird jeweils vor der Adressierung des Speicherbereichs in ein Hilfsregister geladen. Bei jeder Änderung des Dateninhalts des Hilfsregisters wird ein Sperrsignal erzeugt. Mit jedem Ladevorgang des Hilfsregisters wird seitens des Mikroprozessors ein bestimmter Anwender definiert. Greift dieser Anwender auf einen nicht erlaubten Speicherbereich zu, was sich in einer entsprechenden Änderung des Hilfsregisterinhalts auswirkt, erzeugt die Schutzschaltung, die den Inhalt des Hilfsregisters überwacht, ein Sperrsignal.

[0020] Weitere Vorteile und Weiterbildungen der Erfindung ergeben sich aus den Unteransprüchen sowie den Ausführungsbeispielen, die nachfolgend anhand der Figuren beschrieben werden. Darin zeigt

[0021] Fig. 1 einen Datenträger mit integriertem Schaltkreis,

[0022] Fig. 2 ein Blockschaltbild einer für einen Datenträger vorgesehenen integrierten Schaltung mit Mikroprozessor, Speicher und Sperrschialtung,

[0023] Fig. 3 ein Blockschaltbild einer für einen Datenträger vorgesehenen integrierten Schaltung mit einem Arbeitsprozessor und einem Sicherungsprozessor gemäß der Erfindung sowie zugehörigen Speichern und

[0024] Fig. 4 ein Blockschaltbild einer für einen Datenträger vorgesehenen integrierten Schaltung mit Mikroprozessor, Speicher und Sperrschialtung gemäß der Erfindung.

[0025] Fig. 1 zeigt den Aufbau eines Datenträgers, beispielsweise einer Kreditkarte 1 mit Klerschrift-Datenfeld 2, Unterschriftenstreifen 3, und einen in den Kartenkörper eingebetteten integrierten Schaltkreis 5 mit Anschlußkontakten 6. Die Anschlüsse sind hier als Anschlußkontakte 6 in Form von zwei Reihen ausgebildet. Der Aufbau derartiger Karten ist grundsätzlich bekannt und soll hier nicht näher erläutert werden. Ferner ist die Art und Weise des Gebrauchs und die Datenverarbeitung in Verbindung mit solchen Kreditkarten bekannt. Über die Anschlußkontakte 6 erfolgt ein Datenaustausch mit beispielsweise einem Terminal, einem Geldausgabeautomaten oder dergleichen. In der integrierten Schaltung der Kreditkarte werden beispielsweise Sicherheitsroutinen ausgeführt, die für den Berechtigungsnachweis des Kartenbenutzers notwendig sind.

[0026] Fig. 2 zeigt eine integrierte Schaltung, wie sie in der Kreditkarte eingebaut ist. Ein Mikroprozessor 10 enthält eine Steuereinheit 11, die über eine Steuerleitung 18 mit einer Speicheranordnung 30 verbunden ist, eine arithmetisch-logische Einheit (ALU) 12, einen Registersatz 13, ein Adreßregister 14 und ein Datenregister 15. Ein Register des Registersatzes 13 dient als Programmzähler, dessen Inhalt festlegt, auf welche Adresse einer Speicheranordnung 30 zugegriffen wird, um einen Befehl des dort gespeicherten Fremdprogramms abzurufen. Der Befehl veranlaßt beispielsweise, daß aus einer bestimmten Adresse des Speichers ein Datenwert ausgelesen wird. Hierzu wird in dem Adreßregister 14 eine Adresse gespeichert, die beim nächsten Speicherzugriff festlegt, auf welche Adresse zugegriffen wird.

[0027] Die Adresse wird über einen Adreßbus 17 an die Speicheranordnung 30 gegeben. Die in den Speicher 30 eingeschriebenen oder aus dem Speicher 30 ausgelesenen Daten gelangen über einen Datenbus 16 in das Datenregister 15 und von dort in ein Register des Registersatzes 13.

[0028] Die Speicheranordnung 30 umfaßt im dargestellten

Beispiel einen Schreib-/Lesespeicher (RAM) 31, einen Fest-Speicher (ROM) 32 und E²PROM 33. Diese Speicherbereiche 31, 32 und 33 gehören zu dem Betriebssystem (BS), welches zum Teil sicherheitsrelevante Daten enthält, die auf jeden Fall gehalten werden müssen. Um dies zu gewährleisten, ist in dieser einfachen Ausführungsform gemäß Fig. 2 der Zugriff zu sämtlichen Speicherbereichen 31, 32, 33 des Betriebssystems (BS) für einen Anwender aus seinem Fremdprogramm heraus gesperrt.

[0029] Will der Hersteller dem Anwender einen Bereich des Betriebssystems zugänglich machen, der dann selbstverständlich keine sicherheitsrelevanten Daten enthalten darf, so müßte die nachfolgend beschriebene Schutzschaltung 20 in Bezug auf die noch verbleibenden zu schützenden Adressen des Betriebssystems entsprechend angepaßt werden. Indem dem Anwender ein Bereich des Betriebssystems aus seinem Fremdprogramm heraus zugänglich gemacht wird, ist es beispielsweise möglich, ihm die Benutzung zu einer Routine, z. B. zum Vergleich einer eingegebenen Nummernfolge mit einer im Betriebssystem - geschützt - gespeicherten Nummernfolge, zu ermöglichen und ihm hierdurch die Erstellung seines Fremdprogramms zu erleichtern.

[0030] Weiterhin enthält die Speicheranordnung 30 einen Speicherbereich 34 für ein Fremdprogramm. Dieses Fremdprogramm kann von einer Organisation, welche mit dem Hersteller der Karte nicht identisch ist, geladen werden. Hierzu ist der Speicherbereich 34 als E²PROM ausgebildet. Das Fremdprogramm, welches seitens des Anwenders geladen wird, nimmt die Speicherplätze w bis x ein, während das Betriebssystem die Speicherplätze 0 bis w-1 einnimmt.

[0031] Das Fremdprogramm enthält spezielle Routinen und Daten, um beispielsweise festzustellen, ob die von dem Karteninhaber geforderte Dienstleistung, z. B. eine Geldausgabe, zugelassen wird, was beispielsweise vom jeweiligen Kontostand des Karteninhabers abhängt. Nachdem der Karteninhaber die Karte in einen Automaten eingeführt hat, erfolgt ein Datenaustausch zwischen dem Automaten und dem Mikroprozessor 10. Nach der Initialisierung und der Durchführung bestimmter Routinen durch das Betriebssystem kann der weitere Betrieb durch das im Speicherbereich 34 gespeicherte Fremdprogramm erfolgen, beispielsweise dadurch, daß der Programmzähler PC im Registersatz 13 auf die Adresse w eingestellt wird. Damit wird als nächstes der in der ersten Speicherstelle des Speicherbereichs 34 gespeicherte Befehl des Fremdprogramms aufgerufen.

[0032] Um nun zu verhindern, daß seitens des Fremdprogramms auf Adressen in den Speicherbereichen 31, 32 und 33 zugegriffen wird, ist eine erfundungsgemäße Schutzschaltung 20 vorgesehen. Diese Schaltung ist zusätzlich zu dem Mikroprozessor 10 und der Speicheranordnung 30 vorhanden. Vorzugsweise sind alle Komponenten als integrierte Schaltung auf einem einzigen Chip ausgebildet.

[0033] Die Schutzschaltung 20 enthält einen ersten Komparator 21, ein erstes Hilfsregister (HRI) 22, einen zweiten Komparator 23, ein zweites Hilfsregister (HRII) 24, ein UND-Gatter 25 und eine Ausgangsstellung 26, die von dem UND-Gatter 25 zu der Steuerschaltung 11 des Mikroprozessors 10 führt.

[0034] Der Komparator 21 vergleicht die Inhalte des Adreßregisters 14 und des Hilfsregisters 22, während der Komparator 23 den Inhalt des Programmzählers mit dem Inhalt des Hilfsregisters 24 vergleicht.

[0035] Die Inhalte der beiden Hilfsregister 22 und 24 können herstellerseitig in fest verdrahteter Logik "vorprogrammiert" sein. Die Inhalte können auch jeweils im Zuge der Initialisierung des Mikroprozessors durch das Betriebssystem aus gesicherten Speichern in die Hilfsregister geladen werden.

[0036] In das Hilfsregister 22 wird die Adresse w geladen, bei der das Fremdprogramm im Speicherbereich 34 beginnt. Im Hilfsregister 24 wird ebenfalls der Wert w gespeichert. Während der Komparator 21 ein Signal liefert, wenn die im Adreßregister 14 enthaltene Adresse kleiner ist als die im Hilfsregister 22 gespeicherte Adresse w (dies bedeutet, daß das Fremdprogramm auf eine unerlaubte Speicherstelle zwischen 0 und w-1 zugreift), liefert der Komparator 23 ein Signal, wenn der Inhalt des Programmzählers PC des Registersatzes 13 größer oder gleich dem im Hilfsregister 24 gespeicherten Wert w ist, wobei letzteres bedeutet, daß gerade das Fremdprogramm ausgeführt wird.

[0037] Wenn beide Komparatoren 21 und 23 ein Signal liefern, so bedeutet dies, daß das Fremdprogramm ausgeführt und daß auf eine unerlaubte Adresse zugegriffen wird, die außerhalb des Adreßraums des Fremdprogramms liegt. Hierbei liefert das UND-Gatter 25 beispielsweise ein Reset-Signal über die Leitung 26 an die Steuereinheit 11, die dadurch eine weitere Ausführung des Fremdprogramms sperrt.

[0038] Um das Schreiben oder Lesen selektiv zu sperren, wird das Schreib-/Lesesignal des Mikroprozessors in der Schutzschaltung 20 mit verarbeitet (siehe Leitung 27).

[0039] In einer Abwandlung der Ausführungsform gemäß Fig. 2 können zusätzliche Komparatoren mit dazugehörigen Hilfsregister vorgesehen werden, wenn weitere Speicherbereiche für weitere, von verschiedenen Anwendern zu ladende Fremdprogramme vorhanden sind.

[0040] Fig. 3 zeigt eine Ausführungsform der Erfahrung. Ein Arbeitsprozessor 110 mit der dazugehörigen Speicheranordnung (PROM) 130 hat im wesentlichen die gleiche Funktion wie der Mikroprozessor 10 mit der dazugehörigen Speicheranordnung 30 in Fig. 2.

[0041] Als Schutzschaltung dient hier ein zweiter Prozessor, nämlich ein Sicherungsprozessor 120, der eine eigene Speicheranordnung 150 aufweist.

[0042] Ein Betriebstaktsignal Cl legt die Arbeitsgeschwindigkeit des Sicherungsprozessors 120 fest. Über eine Teilerschaltung 140 wird die Frequenz des Taktsignals durch n geteilt, so daß der Arbeitsprozessor 110, der das Ausgangssignal der Teilerschaltung 140 empfängt, nur mit der 1/n-ten Geschwindigkeit arbeitet wie der Sicherungsprozessor 120.

[0043] Der Sicherungsprozessor 120 enthält eine Steuerseinheit 121, die bei Feststellung eines unberechtigten Speicherzugriffs seitens eines Fremdprogramms ein Reset-Signal an den Arbeitsprozessor 110 gibt. Hierzu werden der Adreßbus 117 und die Steuerleitung 111 zwischen dem Arbeitsprozessor 110 und der Speicheranordnung 130 überwacht. Außerdem erfolgt eine Überwachung des Programmzählers (PC) des Arbeitsprozessors. Sowohl die Daten auf dem Adreßbus 117 als auch der Inhalt des Programmzählers PC werden für jedes Fremdprogramm mit bestimmten Grenzwerten verglichen.

[0044] Die Speicheranordnung 130 für den Arbeitsprozessor 110 enthält mehrere Speicherbereiche für verschiedene Anwender, die hier als Anwender I, Anwender II_ bezeichnet sind. Wie oben erwähnt, werden diese Fremdprogramme von einer von dem Kartenhersteller verschiedenen Organisationen separat geladen. Die Speicherbereiche 134, 135 und 136 der Speicheranordnung 130 sind vorzugsweise als nichtflüchtiger Speicher (z. B. E²PROM) ausgebildet.

[0045] Wenn ein bestimmtes Fremdprogramm, z. B. das im Speicherbereich 134 des Anwenders I gespeicherte Programm, von dem Arbeitsprozessor 110 nach erfolgter Initialisierung ausgeführt wird, vergleicht der Sicherungsprozessor 120 die jeweiligen Adresssignale und Programmzähler-Inhalte mit den dazugehörigen Grenzwerten für diesen Anwender. Diese Grenzwerte sind in der Speicheranordnung

150 als Bestandteil des Betriebssystems des Sicherungsprozessors 120 gespeichert. Wenn z. B. das Fremdprogramm des Anwenders I ausgeführt wird, darf der Inhalt des Programmzählers PC nur einen bestimmten Wertebereich abdecken. Außerdem dürfen die Adressen auf dem Adreßbus 117 nur diesem Wertebereich entsprechen. Bei Abweichungen gibt der Sicherungsprozessor 120 das Reset-Signal zum Sperren der Ausführung des Fremdprogramms an den Arbeitsprozessor 110.

[0046] Fig. 4 zeigt eine zweite Ausführungsform der Erfahrung, wobei der dem Mikroprozessor 210 zugeordnete Betriebssystem-Speicher 231 getrennt von den Speicherbereichen 234, 235 und 236 angeordnet sind. Letztere dienen zur Aufnahme von Fremdprogrammen für drei verschiedene Anwender. Zwischen dem Mikroprozessor 210 und den drei Speichern bzw. Speicherbereichen 234, 235, 236 verlaufen Adreß-, Daten- und Steuerbus.

[0047] Der Adreßraum für den Zugriff auf die drei (PROM-)Speicherbereiche 234, 235, 236 umfaßt beispielsweise 16 Bits, wobei die zwei höchstwertigen Bits festlegen, welcher Speicher bzw. welcher Speicherbereich für den aktuellen Zugriff vorgesehen ist. Insgesamt können mit den zwei höchstwertigen Bits vier Speicher oder Speicherbereiche angesprochen werden (00, 01, 10, 11).

[0048] Jeweils vor der Ausführung eines Fremdprogramms wird durch das Betriebssystem, beispielsweise gesteuert durch anwenderspezifische Parameter, in ein erstes Hilfsregister 222 (HRI) ein Wert eingegeben, der im vorliegenden Fall zwei Bit umfaßt. Wenn beispielsweise das Fremdprogramm im Speicher 234 ausgeführt werden soll und dieser Speicher Adressen mit der Bit-Kombination "01" in den zwei höchsten Bit-Stellen aufweist, so wird in das Hilfsregister 222 der Wert "01" eingespeichert.

[0049] Zu Beginn der Ausführung des Fremdprogramms, d. h. mit der ersten Adressierung, werden die beiden höchsten Stellen des Adreßregisters von dem Adreßbus in ein zweites Hilfsregister (HRI) 223 geladen und ein die Inhalte der beiden Hilfsregister 222 und 223 vergleichender Komparator 221 durch ein entsprechendes Steuersignal 228 des Mikroprozessors aktiviert. Solange der Inhalt des Hilfsregisters 222 mit dem Hilfsregister 223 übereinstimmt, bedeutet dies, daß sich das Fremdprogramm lediglich in dem ihm zugeordneten Adreßraum (Speicherbereich 234) bewegt. Wird auf einen anderen Adreßraum zugegriffen, so ändern sich damit die beiden höchsten Stellen des Adreßsignals und damit der Inhalt des Hilfsregisters 223. Dies wird von dem Komparator 221 festgestellt, der über eine Leitung 226 ein Reset-Signal an den Mikroprozessor 210 gibt.

Patentansprüche

1. Kartenförmiger Datenträger mit datenschützender Mikroprozessorschaltung zur Verhinderung des Zugriffs auf in Speichern abgelegten Daten oder Programmen mit einem Arbeitsprozessor, einem Speicher für ein Betriebssystem und mehreren Speicherbereichen zur freien Programmierung mit jeweils einem individuellen Fremdprogramm, mit einer Schutzschaltung, bestehend aus einer ersten Einrichtung zur Überwachung der jeweils gültigen Zugriffadresse, einer zweiten Einrichtung zur Überwachung des jeweiligen Inhalts des Arbeitsprozessor-Programmzählers und einer dritten Einrichtung, die die Signale der Überwachungseinrichtungen zur Erzeugung eines Sperrssignals verknüpft, dadurch gekennzeichnet, daß die Schutzschaltung ein zweiter Mikroprozessor ist, der mit der gleichen oder einer höheren Taktfrequenz betreibbar ist als der Ar-

DE 41 15 152 C 2

7

8

beitsprozessor.

2. Kartenförmiger Datenträger nach Anspruch 1, dadurch gekennzeichnet, daß das Sperrsignal der Verknüpfungseinrichtung auf den Interrupt-Eingang des Arbeitsprozessors geführt wird.

3. Kartenförmiger Datenträger nach einem oder mehreren der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß das Sperrsignal der Verknüpfungseinrichtung auf den Reset-Eingang des Arbeitsprozessors geführt wird.

4. Kartenförmiger Datenträger nach einem oder mehreren der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß der zweite Mikroprozessor und der die Fremdprogramme steuernde Arbeitsprozessor auf dem gleichen integrierten Schaltkreis angeordnet sind.

5. Kartenförmiger Datenträger nach einem oder mehreren der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß dem zweiten Mikroprozessor ein Grenzwertspeicher zugeordnet ist, in welchem Grenzwerte für die überwachten Adressen und für mögliche Inhalte des Programmzählers des Arbeitsprozessors gespeichert sind, auf die der Arbeitsprozessor keine Zugriffsmöglichkeit hat.

6. Kartenförmiger Datenträger mit datenschützender Mikroprozessorschaltung zur Verhinderung des Zugriffs auf in Speichern abgelegten Daten oder Programmen mit einem Arbeitsprozessor, mit einem Speicherbereich für ein Betriebssystem und mehreren Speicherbereichen zur freien Programmierung mit jeweils einem individuellen Fremdprogramm, wobei die Adressräume der Speicherbereiche wenigstens in den zwei höchstwertigen Stellen gleich sind, mit einem ersten Hilfsregister, in dem die höchstwertigen Stellen des Adressraumes des auszuführenden Fremdprogramms abgelegt sind, mit einem zweiten Hilfsregister, in dem die höchstwertigen Stellen der jeweiligen ZugriffAdresse abgelegt sind, mit einem Komparator zum Vergleich der Inhalte der beiden Hilfsregister, der ein Sperrsignal erzeugt, wenn die Inhalte der Hilfsregister nicht übereinstimmen.

5

10

15

20

25

30

35

40

45

50

55

60

65

Hierzu 2 Seite(n) Zeichnungen

- Leerseite -

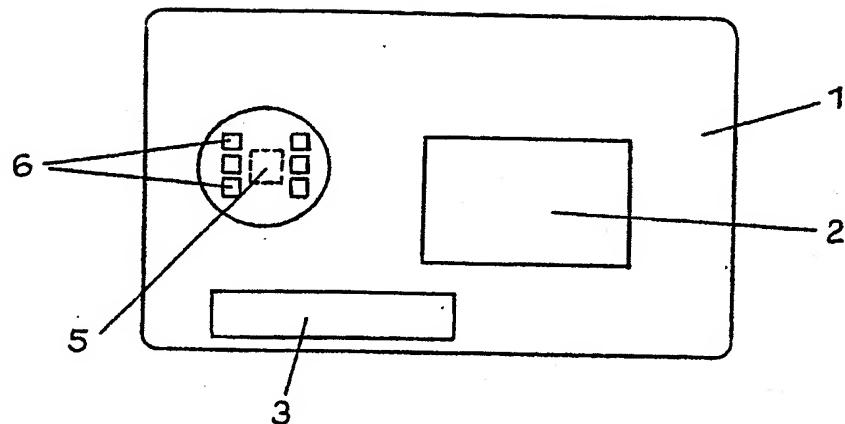


Fig. 1

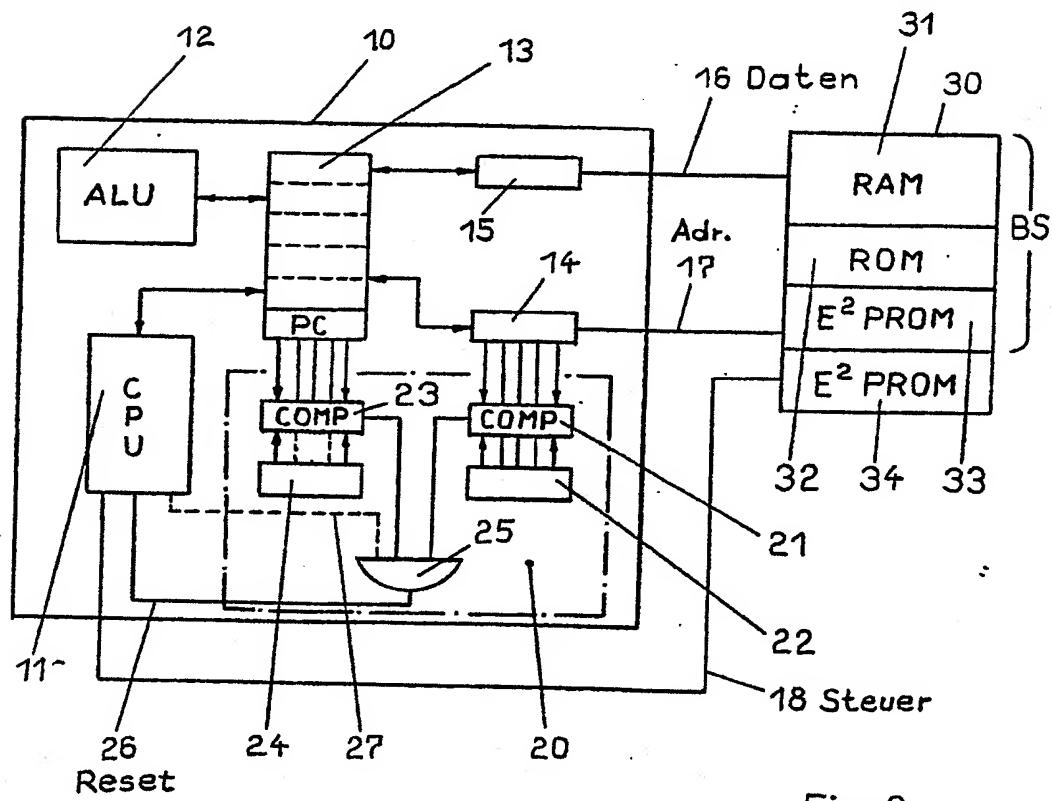


Fig. 2

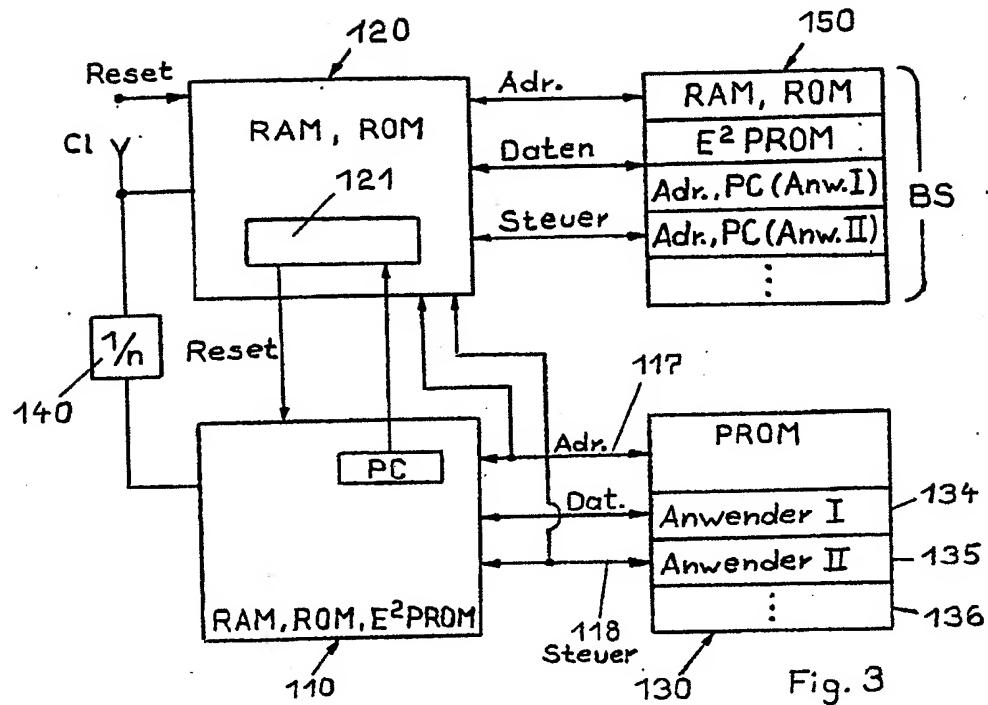


Fig. 3

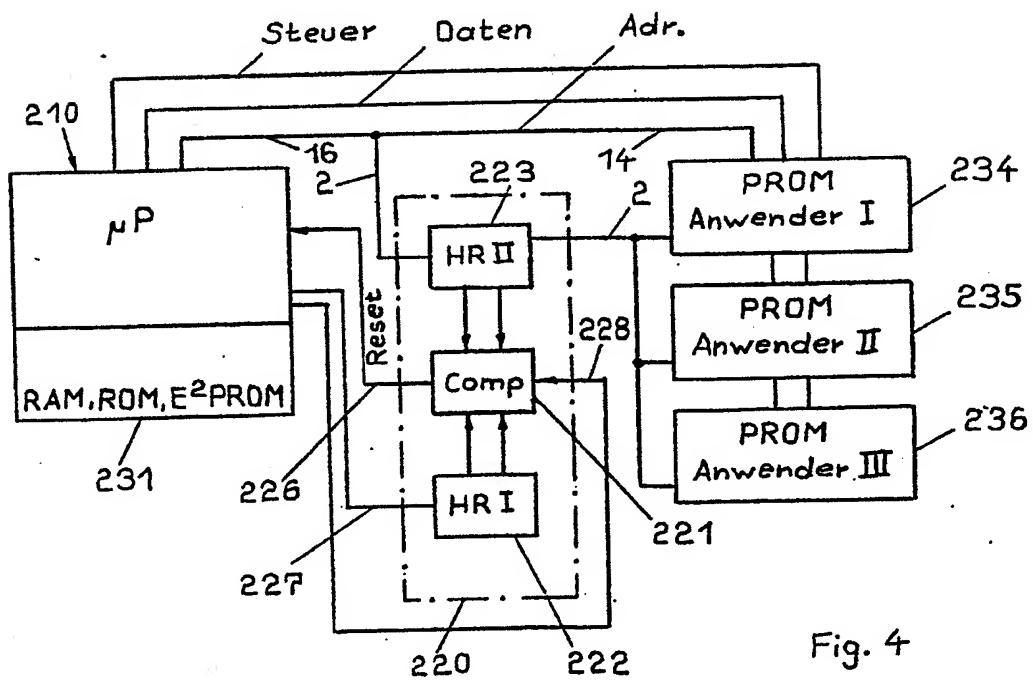


Fig. 4